TECHNISCHE UNIVERSITÄT DARMSTADT

Technische Universität Darmstadt
Department of Computer Science
Chair of Applied Cryptography

Master Thesis

Incoercible Sale

Longer subtitle (if required)

Nikolaos Stivaktakis

September 26, 2019

Supervisors: Prof. Sebastian Faust, Ph.D.
2nd supervisor

Abstract

Write an abstract

!!! Prüfen Sie, dass der folgende Text aktuell ist (entsprechend der formalen Regeln des Studienbüros) !!!
!!! Check that this text is up to date (according to formal rules of the examination office) !!!

Erklärung zur Abschlussarbeit gemäß § 22 Abs. 7 APB TU Darmstadt

Hiermit versichere ich, **Nikolaos Stivaktakis**, die vorliegende Master-Thesis / Bachelor-Thesis gemäß § 22 Abs. 7 APB der TU Darmstadt ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
Mir ist bekannt, dass im Falle eines Plagiats (§38 Abs.2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5,0 bewertet und damit ein Prüfungsversuch verbraucht wird. Abschlussarbeiten dürfen nur einmal wiederholt werden.
Bei einer Thesis des Fachbereichs Architektur entspricht die eingereichte elektronische Fassung dem vorgestellten Modell und den vorgelegten Plänen.

English translation for information purposes only: Thesis Statement pursuant to § 22 paragraph 7 of APB TU Darmstadt

I herewith formally declare that I, **first name last name**, have written the submitted thesis independently pursuant to § 22 paragraph 7 of APB TU Darmstadt. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I clearly marked and separately listed all of the literature and all of the other sources which I employed when producing this academic work, either literally or in content. This thesis has not been handed in or published before in the same or similar form.
I am aware, that in case of an attempt at deception based on plagiarism (§38 Abs. 2 APB), the thesis would be graded with 5,0 and counted as one failed examination attempt. The thesis may only be repeated once.
For a thesis of the Department of Architecture, the submitted electronic version corresponds to the presented model and the submitted architectural plans.

Datum / Date

Unterschrift / Signature

Contents

1 Introduction

2 Preliminaries

2.1 Cryptography

2.2 Game Theory

2.3 Blockchains

2.4 Smart Contracts

2.5 Escrows

3 Related work

3.1 first escrowless protocol

Zimbeck mit Bithalo auch die analyse erwähnen

3.2 digital vs Physical

Hier unbedingt Asganokar sein paper erwähnen (sale of digital goods)

4 Formalization

4.1 Entities

Seller
An entity that owns a specific physical good G. The seller has bigger utility in owning P amount of coins in contrast to owning G. He therefore desires to exchange G against coins of amount P.

Buyer
An entity that owns coins of at least amount of P. The Buyer has greater utility in owning G in contrast to owning P amount of coins. He therefore desires to exchange coins of amount P against G.

Escrow/Smart Contract
An entity that should ensure that the trade is successful. It acts as a fully trusted oracle.

Helper Box
Fully trusted by Buyer. //need to expand on that

4.2 The Game

Start Point
A Seller and a buyer want to trade successfully: Both have funds in the given cryptocurrency. The seller is in possession of the physical good.

End Point
The buyer is in possession of the physical good and his funds have decreased by amount p. The funds of the seller have increased by p.

Assumptions
Both entities have access to the Escrow and know the addresses of each other. The seller also knows the physical address to which the buyer wants the good to be shipped. Other than this information they know nothing about each other.
Both parties can send funds in the given cryptocurrency to any address. The sender has the power to send/ship the physical good to any physical address he wants. The Escrow is a smart contract and both the seller and the buyer know the code of the Smart Contract.
We assume both entities to behave rational, meaning that they both want to maximise their expected payoff.
Transaction Fees and Fees for the escrows are not analysed.

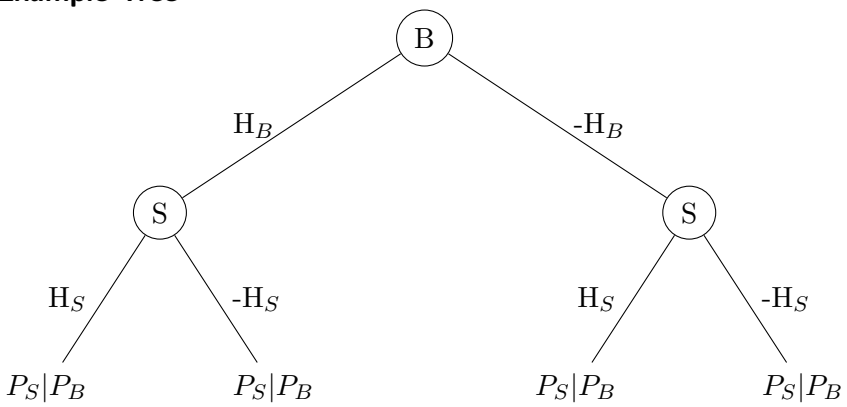
Success of the trade
The trade is considered successful, if the situation transitions from the start point to the end point.

Goal
The goal is to design the Escrow in such a way, that it is the best strategy for both the buyer and the seller to perform a successful trade. That means that a successful trade should be the Nash Equilibrium.

5 Proposed Possible Solutions

To analyse turn based games I will use Game trees.

Example Tree



Description
To analyse Simultaneous games I will use a table.

Example table

	H_B	$-H_B$
H_S	$P_S\|P_B$	$P_S\|P_B$
$-H_S$	$P_S\|P_B$	$P_S\|P_B$

Description
On the top are the possible strategies for the buyer: H_B is the strategy where the buyer behaves honestly and $-H_B$ is the strategy where the Buyer behaves dishonestly.
On the left side are the strategies for the seller. Similar to the buyer, H_S denotes the strategy where the seller behaves honestly and $-H_S$ denotes the strategy where the seller behaves dishonestly.

For each combination of strategies the two parties get a specific payout. P_S denotes the payoff of the seller and P_B denotes the payoff of the buyer.

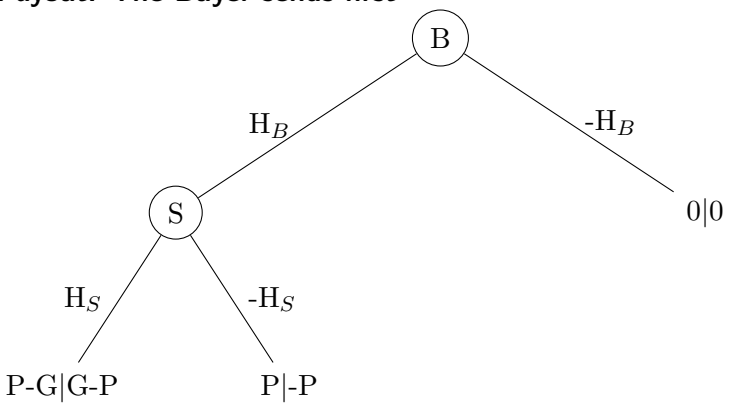
5.1 The naive approach

To examine any possible solutions, we begin with the simplest possible protocol.
The simplest protocol is without collateral and any third party. In this case there are 3 possibilities:

- First the buyer sends coins of amount P to the seller and then the seller ships the physical good G to the provided address.
- First the seller ships the physical good G to the provided address and then the buyer sends coins of amount P to the seller.
- Both parties send the resources simoultaneously

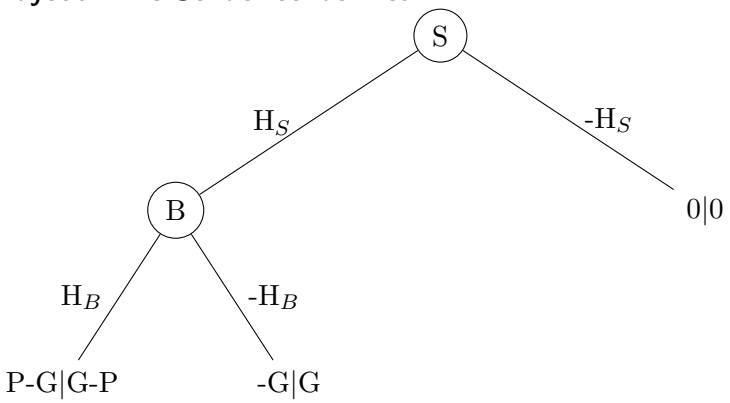
the following: The buyer sends coins of amount P to the seller and then the seller ships the physical good G to the provided address. There is no third party involved.

Payout: The Buyer sends first



To analyze the payout, we start at the bottom at the seller's decision. As he would choose the option, which yields him the greatest payoff, he chooses -H_S (P+G > P).
Therefore the Buyers has to choose between a payoff of 0 (by choosing -H_B) and -P (by choosing H_B). Since 0 > -P, he chooses -H_B.
The Nash Equilibrium of this game is {-H_S, -H_B} and results in a Payoff of 0|0. Both parties are not sending anything and the trade is unsuccessful.

Payout: The Sender sends first



The analysis is similar to the above case, but the roles are reversed. The Buyer would choose -H_B as G > G-P.
The sender would choose -H_S as 0 > -G.
The Nash Equilibrium of this game is {-H_S, -H_B} and results in a Payoff of 0|0. Again, both parties are not sending anything and the trade is unsuccessful.

Payout: Both parties send simultaneous

	H_B	-H_B
H_S	$P-G\|G-P$	$-G\|G$
-H_S	$P\|-P$	0|0

If we look at the payoff table we can see that -H_B dominates H_B and -H_S dominates H_S. This means that the dishonest strategy provides a bigger payoff regardless of the strategy of the other party.
Since we assume the players to be rational, they would both chose the dishonest strategy. Both players choosing the dishonest strategy is the Nash Equilibrium of the game.
It is interesting to note that this table resembles the famous prisoner's dilemma. The Nash Equilibrium is on both parties not sending anything, still it would be better for both parties, if they just traded honestly.

5.2 One Side collateral

To incentivize an entity to behave honestly we introduce collateral. The collateral will be lost, if the entity does not behave honestly. In this section I will look at protocols, where only one entity deposits a collateral.

5.2.1 Buyer Collateral

Following protocol is proposed:

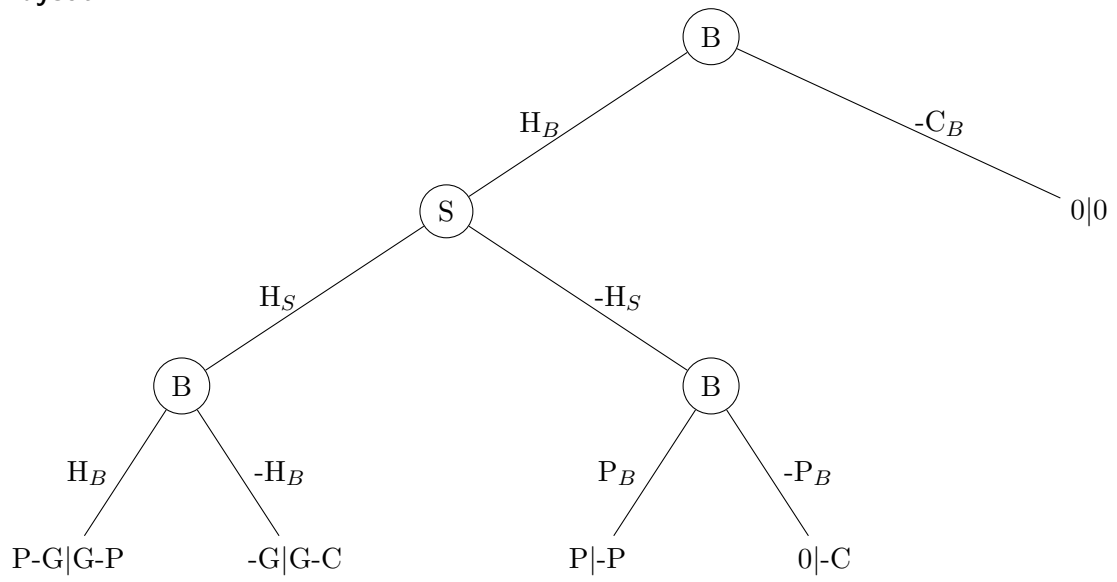
1. Buyer deposits collateral $C > P$ to the Smart Contract
2. Seller sends physical good G to the seller
3. After receiving G, the Buyer sends funds of amount P to the seller
4. The Smart Contract releases the collateral of the Buyer

Because the Smart Contract has access to the blockchain, it can automatically release the collateral if the Buyer sends P to the seller. The collateral should incentivize the Buyer to pay the seller after receiving the physical good G.

Possible Strategies

With this new protocol there are new possible strategies. Of course there is still the honest strategy for both players, where they behave according to the protocol description. With this strategy the trade unravels successfully.
But there exist other strategies: The dishonest strategy is again not sending the resources. This strategy is denoted as -H_B (when the buyer does not send the coins) and -H_S (when the seller does not send the physical good.
The Seller has also a third possible strategy: Since he decides what happens to the collateral, he can coerce the Buyer into sending him extra resources. This strategy will be denoted C_S. When the seller uses strategy C_S, he does not send the physical good. He rather sends a message to the Buyer: "I will not send you the physical good. Since your collateral is locked and it will only be released if you pay me P, I propose the following deal: In spite of me not sending you G, you still send me P and you get back your collateral, as it "
-C is not depositing the collateral.
P is paying P although S deviates, -P is not paying when S deviates.

Payout



	H_B	$-H_B$
H_S	$P \mid G$	$0 \mid G + P - C$
$-H_S$	$G + P \mid 0$	$G \mid P - C$

The biggest possible payout for the Seller is if he can coerce the Buyer into sending him additional $\frac{P}{2}$ coins. This happens when the seller is choosing strategy C_S and the buyer strategy $-H_B$. It should be noted, that when the seller tries to coerce the buyer (C_S), it is actually his best option to comply ($-H_B$). This scenario is the Nash Equilibrium, because choosing a different strategy only results in a lower payoff for the player, if the other player is keeping his strategy.
The Nash Equilibrium would result in a payoff of $G + \frac{P}{2}$ for the Buyer and a payoff of $\frac{P}{2}$ for the seller. The rational buyer would never initiate the trade, because this trade will always result in a loss, if the seller behaves rational.

5.2.2 Seller Collateral

Following protocol is proposed:

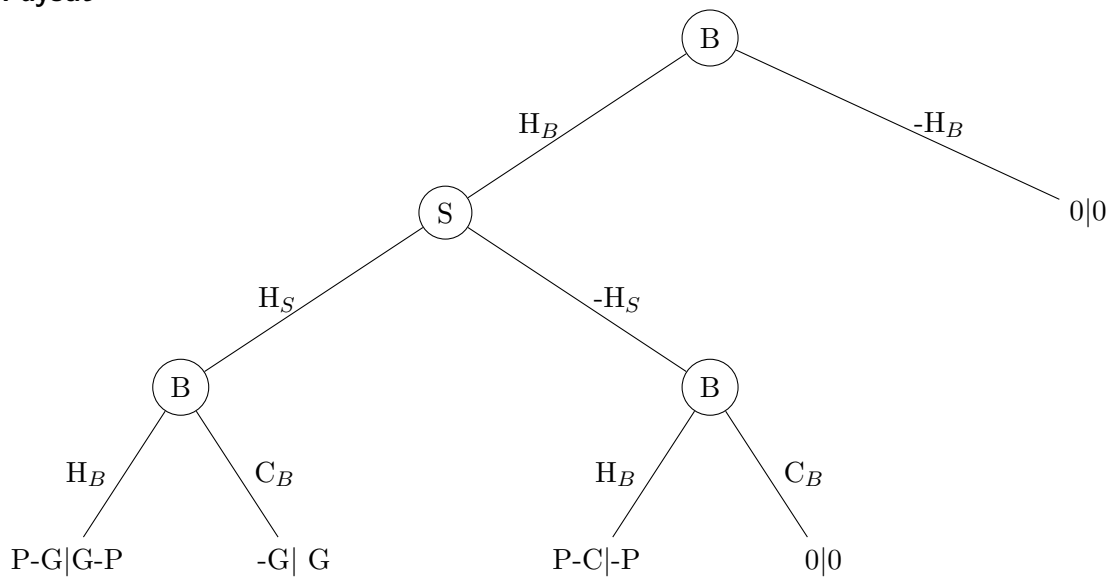
1. Seller deposits collateral $C > P$ to the Smart Contract
2. Buyer sends funds of amount P to the seller
3. Seller sends the physical good to the Buyer
4. Buyer receives the physical good and confirms it to the Smart Contract
5. The Smart Contract releases the collateral of the Seller

The collateral should incentivize the Seller to behave honestly and to ship the physical good to the buyer.

Possible Strategies

There is still the honest strategy (H_S, H_B) for both players, where they behave according to the protocol description. With this strategy, the trade still unravels successfully.
The dishonest strategy is again not sending the resources. This strategy is still denoted as $-H_B$ (when the buyer does not send the coins) and $-H_S$ (when the seller does not send the physical good.
The Buyer has also a unique opportunity: Since he decides what happens to the collateral, he can coerce the Seller into sending him extra resources. This strategy will be denoted C_B. After receiving the physical good he can tell the Seller: "Either you send me back my payment P or I will tell the Smart Contract that you did not send me the physical good." In this case it is best for S to comply, because $C > P$.

Payout



Normally there is another layer under C$_B$: Does S comply and send P or not? As already discussed, it is always better for the seller to send back the payment P and recieve back his collateral C, because $C > P$. Should I put it in the tree? make it bigger and more difficult to read but completely correct.

	H$_B$	-H$_B$	C$_B$
H$_S$	$P\|G$	$G\|P$	$0\|G+P$
-H$_S$	$P+G-C\|0$	$G\|P$	$G\|P$

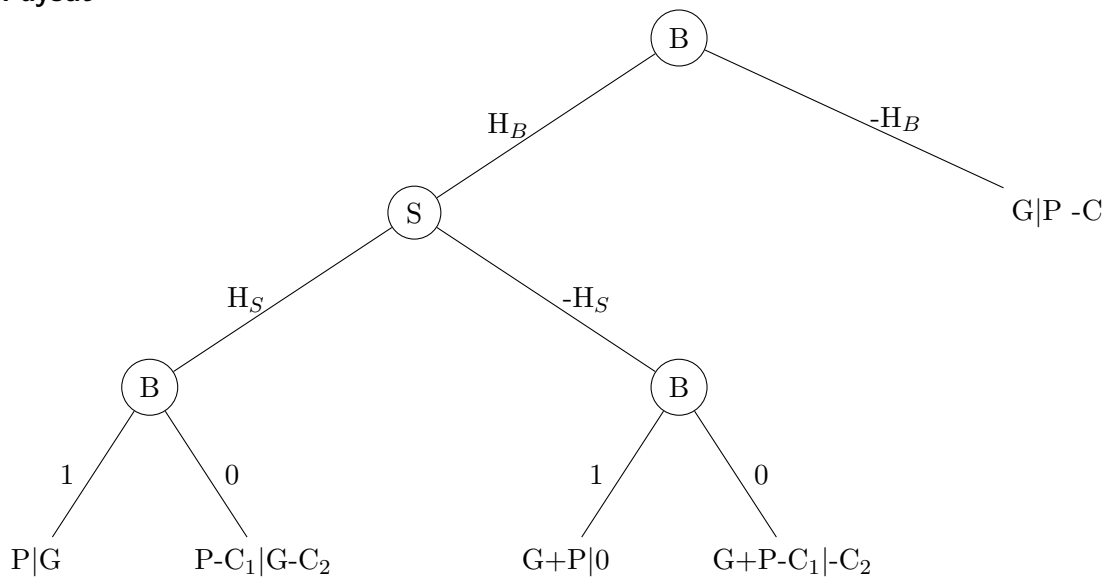
If B sends the coins (does not choose strategy -H$_B$), S has to make the following decision: Does he send the good (H$_S$) or not (-H$_S$)? We have to take into account, that B decides what happens with the collateral.
What was designed to be an incentive for S to behave honestly, ended up as leverage for B over S. B can report 0 (and burn the collateral) even if S behaves honestly. Since sending the good has no impact on the collateral (the rational buyer will always play strategy C$_B$ over H$_B$), it is best for S to not send the physical good (-H$_B$). Because not Sending (-H$_S$) is the best strategy for the seller, it is best for B to not even send P and therefore not engage in the trade at all (-H$_B$).
The Nash Equilibrium would be in nobody sending anything and the trade not happening.

5.3 Two Side Collateral

Following protocol is proposed:

1. Seller deposits collateral $C_1 > P$ to the Smart Contract
2. Buyer deposits collateral $C_2 > P$ to the Smart Contract
3. Buyer sends Funds of amount P to the Seller
4. Seller sends physical good G to the seller
5. Buyer receives the physical good and confirms it to the Smart Contract
6. The Smart Contract releases the collateral of the Seller and the Buyer

Payout



5.4 SC 5/6 innputs What is a nice Headline for this section??

5.4.1 Ideal Funcionality

We can model the ideal funcionality of our Smart Contract as a Function with 6 inputs and 2 outputs:

Inputs

- Int: Buyer Collateral DO WE REALLY NEED THAT as input?
- Int: Seller Collateral DO WE REALLY NEED THAT as input?
- Int: the Price P
- Bool: Sellers report
- Bool: Buyers report
- Bool: Was the physical good G shipped by the seller?

Inputs MAYBE EASIER

- Int: agreed price P
- Bool: Was the physical good G shipped by the seller?

Idea: the Smart Contract automatically collects (instructs the entities to make a deposit) of the right amount. If the physical good was shipped, he transfers P to the Seller, else he gives back the inital deposit to both parties

Outputs

- Int: Buyer Payout
- Int: Seller Payout

$$SC_{ideal} := .... \tag{5.1}$$

Functionality

The function will always output the right amount to the two entities:

- It cuts the collateral of all lying parties
- It will give the amount of P to the seller, if he actually ships the physical good G, otherwise give it back to the seller

Such a smart contract solves the problem completely as the Nash Equilibrium is both parties behaving honestly.It resembles the case of shipping a digital verifiable good.

5.4.2 Real World Functionality

In the real world, the smart contract does have the last input. The Smart Contract has no way of knowing, if the physical good was actually shipped or not.
This poses following problem: There are cases where the input to the ideal functionality differs only by the last input (if the seller actually sent the good), but the output to the two party differs vastly. These two cases are indistinguishable if the last input is missing. Therefore it is not possible for a function with only the five inputs to have the ideal outputs.

5.5 Possible Proof

Since behaviour of the smart contract is only influenced by the transactions of the two parties, we can model the payoff to each party with a function that just takes the transactions as input:

$$SC(Tx_1, Tx_2, ..., Tx_n) = (P_B, P_S) \tag{5.2}$$

Since we assume only these two players, each transaction has to be made either from the buyer or from the seller.

Let us assume we design a situation where the Nash Equilibrium is for both parties to behave honestly and the trade to unravel successfully. In the honest case, the Transactions sent to the SC are denoted as $\text{Tx}_{honestSeller}$ for the sellers transactions and $\text{Tx}_{honestBuyer}$ for the Buyers transactions.
As the honest case is the Nash Equilibrium, the sender gets a higher payout when he sends the good in comparison when he is dishonest and keeps the good to himself.

$$P_{honestSeller} > P_{dishonestSeller} \tag{5.3}$$

Payoff honest seller

$$P_{honestSeller} = P_{SC}(S_{honest}) - U_S(G) \tag{5.4}$$

$P_{SC}(S_{honest})$ is the amount of coins that the seller gets from the smart Contract. As the honest seller sends G to the buyer, his payoff decreases by $U_S(G)$

Payoff dishonest seller

$$P_{dishonestSeller} = P_{SC}(S_{dishonest}) \tag{5.5}$$

As the dishonest seller does not send the item, his payoff is exactly the amount of coins that he gets from the smart contract.

The smart contract has to change the payoff
from (5.3), (5.4),(5.5):

$$P_{SC}(S_{honest}) - U_S(G) > P_{SC}(S_{dishonest}) \tag{5.6}$$

The amount of coins, that a honest seller gets back has to be substantially more than the amount of coins that a dishonest seller gets back.
Since the payoff from the SC is only dependent on the transaction of the two players, at least one of the two players has to change at least one transaction (from the honest case), so that the SC can detect that the seller is dishonest and return the different payouts.

The Buyer has to have a set of transaction $\text{Tx}_{penalizeSeller}$, in which he can decrease the sellers payoff to under $P_{SC}(S_{honest}) - U_S(G)$, as described in (5.6).
This transactions have to be unstoppable, meaning that there exist no set of transactions $\text{Tx}_{cheatingSeller}$ for the seller, such that his payoff stays above $P_{SC}(S_{honest}) - U_S(G)$.
If such a set of transaction would exist, he would not send the item and post $\text{Tx}_{cheatingSeller}$. His Payoff would be

$$P_{cheatingSeller} = P_{SC}(Tx_{cheatingSeller}) > SC(S_{honest}) - U_S(G) = P_{honestSeller}$$

This would break our assumption, that the Nash Equilibrium is when both players behave honestly.

To summarize: The Buyer has to have a set of transactions that decrease the payoff from the SC to the seller to under $P_{SC}(S_{honest}) - U_S(G)$, NO MATTER what transactions the seller posts.
Since we assume a rational Buyer, for him to post $\text{Tx}_{cheatingSeller}$, he has to get a bigger payout:

$$P_B(Tx_{cheatingseller}) > P_B(Tx_{honestBuyer})$$

Now he has a set of transactions, that increase his payoff. He could post these transactions, even if the seller behaves honestly and sends the good.
This contradicts our assumption that the Nash Equilibrium is when both players behave honestly.

6 Open Research/ Questions

7 Conclusion